Calendar No. 252

109TH CONGRESS
1ST SESSION

S. 1326

To require agencies and persons in possession of computerized data containing sensitive personal information, to disclose security breaches where such breach poses a significant risk of identity theft.

IN THE SENATE OF THE UNITED STATES

JUNE 28, 2005

Mr. SESSIONS introduced the following bill; which was read twice and referred to the Committee on the Judiciary

OCTOBER 20, 2005

Reported by Mr. SPECTER, without amendment

A BILL

To require agencies and persons in possession of computerized data containing sensitive personal information, to disclose security breaches where such breach poses a significant risk of identity theft.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Notification of Risk to Personal Data Act''.

SEC. 2. DEFINITIONS.

In this Act, the following definitions shall apply:

(1) AGENCY.—The term ''agency''—

(A) has the meaning given such term in section 551(1) of title 5, United States Code; and

(B) includes any authority of a State or political subdivision.

(2) BREACH OF SECURITY OF THE SYSTEM.—The term ''breach of security of the system''—

(A) means the compromise of the security of computerized data containing sensitive personal information that establishes a reasonable basis to conclude that a significant risk of identity theft to an individual exists; and

(B) does not include the compromise of the security of computerized data, if the agency or person concludes, after conducting a reasonable investigation, that there is not a significant risk of identity theft to an individual, including a situation in which—

(i) sensitive personal information is acquired in good faith by an employee or agent of the agency or person and the information is not subject to further unauthorized disclosure;

(ii) an investigation by an appropriate law enforcement agency, government agency, or official determines that there is not a significant risk of identity theft; or

(iii) the agency or person maintains or participates in a security program reasonably designed to block unauthorized transactions before they are charged to an individual's account and the security program does not indicate that the compromise of sensitive personal information has resulted in fraud or unauthorized transactions.

(3) PERSON.—The term ''person'' has the meaning given such term in section 551(2) of title 5, United States Code.

(4) SENSITIVE PERSONAL INFORMATION.—The term ''sensitive personal information''—

(A) means—

(i) an individual's first and last name;

(ii) the individual's address or telephone number; and

(iii) the individual's social security number, the individual's driver's license number or equivalent State identification number, or the individual's financial ac-

count number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account, if the data element under this clause is not encrypted or redacted and is linked to the information described in clauses (i) and (ii); and

(B) does not include—

(i) any list, description, or other grouping of individuals (and publicly available information pertaining to them) that is derived without using any sensitive personal information; or

(ii) publicly available information that is lawfully made available to the general public from Federal, State or local government records.

(5) REDACTED.—The term ''redacted'' means truncated so that not more than the last 4 digits of the social security number, driver's license number, State identification card number, or account number are accessible as part of the data.

(6) IDENTITY THEFT.—The term ''identity theft'' means a fraud committed using the identifica-

tion of another person with the intent to commit, or to aid or abet any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law and that results in economic loss to the individual.

(7) PERSONAL INFORMATION.—The term ''personal information'' means personally identifiable information about a specific individual.

(8) FUNCTIONAL REGULATOR.—The term ''functional regulator'' means—

(A) the Office of the Comptroller of the Currency with respect to national banks, and Federal branches, Federal agencies of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers);

(B) the Board of Governors of the Federal Reserve System with respect to member banks of the Federal Reserve System (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, organizations oper-

ating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601 and 611), bank and financial holding companies, and any nonbank subsidiaries or affiliates of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers);

(C) the Board of Directors of the Federal Deposit Insurance Corporation with respect to banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System), insured State branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers);

(D) the Director of the Office of Thrift Supervision with respect to savings association the deposits of which are insured by the Federal Deposit Insurance Corporation, savings and loan holding companies, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers);

(E) the National Credit Union Administration Board with respect to any Federal credit union and any subsidiaries of such an entity;

(F) the Secretary of Transportation with respect to any air carrier or foreign air carrier subject to part A of subtitle VII of title 49, United States Code;

(G) the Secretary of Agriculture with respect to any activities subject to the Packers and Stockyards Act, 1921 (7 U.S.C. 181 et seq.) (except as provided in section 406 of that Act (7 U.S.C. 226 and 227));

(H) the Farm Credit Administration with respect to any Federal land bank, Federal land bank association, Federal intermediate credit bank, or production credit association;

(I) the Securities and Exchange Commission with respect to any broker or dealer, investment company or investment adviser;

(J) the applicable State insurance authority of the State in which the person is domiciled with respect to any person engaged in providing insurance;

(K) the Federal Communications Commission with respect to any entity subject to the jurisdiction of the Commission; and

(L) the Federal Trade Commission with respect to any other financial institution or other person that is not subject to the jurisdiction of any agency or authority under subparagraphs (A) through (K).

SEC. 3. DATABASE SECURITY.

(a) IN GENERAL.—Any agency or person that owns or licenses computerized data containing sensitive personal information shall implement and maintain reasonable security and notification procedures and practices appropriate to the size and nature of the agency or person and the nature of the information to protect the sensitive personal information from unauthorized access, destruction, use, modification or disclosure.

(b) DISCLOSURE OF SECURITY BREACH.—

(1) NOTIFICATION OF INDIVIDUAL.—

(A) IN GENERAL.—If an agency or person that owns or licenses computerized data containing sensitive personal information, determines, after discovery and a reasonable investigation, or notification under paragraph (2), that a significant risk of identity theft exists as

a result of a breach of security of the system of such agency or person containing such data, the agency or person shall notify any individual whose sensitive personal information was compromised if such individual is known to be a resident of the United States.

(B) DELAY OF NOTIFICATION.—If a Federal law enforcement agency of either appropriate domestic or foreign jurisdiction determines that the notification required under this subsection would impede a criminal or civil investigation, such notification may be delayed until such Federal law enforcement agency determines that the notification will no longer compromise such investigation.

(2) NOTIFICATION OF OWNER OR LICENSOR.—Any agency or person in possession of computerized data containing sensitive personal information that the agency or person does not own or license shall notify the entity from whom it received the information if the security of the sensitive personal information was compromised and such compromise has resulted in a significant risk of identity theft to an individual.

(3) TIMELINESS OF NOTIFICATION.—All notifications required under paragraph (1) or (2) shall be made as expediently as possible and without unreasonable delay following—

(A) the discovery and reasonable investigation by the agency or person of a breach of security of the system; and

(B) any measures the agency or person takes that are necessary to determine the scope of the breach, prevent further breaches, determine whether there is a reasonable basis to conclude that a significant risk of identity theft to an individual exists, restore the reasonable integrity of the data system, and comply with applicable requirements of securities laws and regulations.

(4) METHODS OF NOTICE.—An agency or person shall be in compliance with this subsection if it provides the resident, owner, or licensee, as appropriate, with—

(A) written notification to a mailing address for the subject individual;

(B) telephonic notification to a telephone number for the subject individual;

(C) e-mail notice to an e-mail address for the subject individual; or

(D) conspicuous posting of the notice on the Internet site of the agency or person, if the agency or person maintains an Internet site, or notification to major media, if—

(i) the agency or person demonstrates that the cost of providing direct notice under paragraphs (A) through (C) of this subsection would exceed $250,000;

(ii) the affected class of subject individuals to be notified exceeds 500,000; or

(iii) the agency or person does not have sufficient contact information for those to be notified.

(5) CONTENTS OF NOTICE.—Notice under this subsection shall—

(A) be given in a clear and conspicuous manner;

(B) describe the breach of security of the system in general terms and the type of sensitive personal information involved; and

(C) include a toll-free telephone number or website that individuals can utilize for further information and assistance.

(6) DUTY TO COORDINATE WITH CONSUMER REPORTING AGENCIES.—Before any agency or person provides notice to more than 1,000 individuals at any time, or provides notice pursuant to paragraph (4)(D), that sensitive personal information on the individuals was, or may reasonably be expected to have been, the subject of a breach of security of the system, the agency or person shall, without unreasonable delay—

(A) notify all nationwide consumer reporting agencies (as defined in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p))) of the timing, content, and distribution of the notice, including—

(i) the number of individuals to whom the notice will be given; or

(ii) the type of notice provided under paragraph (4)(D); and

(B) conform the notice to individuals to be delivered by such agency or person to accurately reflect, to the extent given in such notice—

(i) the method of contact reasonably specified by each nationwide consumer reporting agency that such individuals are to

use with respect to the particular notice; and

(ii) the responsibilities of a nationwide consumer reporting agency under the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) and any other applicable law.

(7) SAFE HARBOR.—Notwithstanding any other obligation under this subsection, an agency or person that maintains notification procedures as part of an information security policy for the treatment of sensitive personal information and is otherwise consistent with the requirements of paragraphs (3) and (6) shall be in compliance with this subsection if the agency or person notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(8) RELATION TO OTHER PROVISIONS.—Nothing in this Act shall be construed to modify, limit or supersede the operation of either the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, or any other applicable provision of Federal law.

(c) CIVIL REMEDIES.—

(1) PENALTIES.—

(A) IN GENERAL.—Except as provided under subparagraph (B), any agency or person

that fails to give notice in accordance with paragraph (1) through (4) of subsection (b) shall be subject to—

(i) a fine in an amount not to exceed $250,000 per breach of security of the system; or

(ii) in the case of a violation of subsection (a), such actual damages as may be proven.

(B) EXEMPTION.—An agency or person shall not be subject to a fine under this paragraph if the breach of security of the system—

(i) was not a result of the negligence of such agency or person; and

(ii) was the result of fraud committed by a third party.

(2) EQUITABLE RELIEF.—Any person that violates, proposes to violate, or has violated this section may be enjoined from further violations by a court of competent jurisdiction.

(3) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this subsection are cumulative and shall not affect any other rights and remedies available under law.

(d) ENFORCEMENT.—

(1) IN GENERAL.—The functional regulator is authorized to enforce compliance with this section, including the assessment of fines under subsection (c)(1).

(2) CIVIL ACTIONS.—No private right of action or class action shall be brought under this Act. No person other than the attorney general of a State may bring a civil action under the law of any State if such action is premised in whole or in part upon the defendant violating any provision of this Act.

SEC. 4. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) IN GENERAL.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any person in a practice that is prohibited under this Act, the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a United States district court of appropriate jurisdiction to—

(A) enjoin that practice;

(B) enforce compliance with this Act; or

(C) obtain damage, restitution, or other compensation on behalf of residents of the

State under the conditions and up to the monetary limits set forth in section 3(c)(1).

(2) NOTICE.—

(A) IN GENERAL.—Before filing an action under paragraph (1), the attorney general of the State shall provide the Attorney General of the United States and the functional regulator—

(i) written notice of the action; and

(ii) a copy of the complaint for the action.

(B) EXEMPTION.—

(i) IN GENERAL.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the State attorney general determines that it is not feasible to provide the notice described in such subparagraph before the filing of the action.

(ii) NOTIFICATION.—In an action described in clause (i), the attorney general of a State shall provide notice and a copy of the complaint to the functional regulator and the Attorney General at the time the State attorney general files the action.

(C) UNITED STATES ATTORNEY GENERAL PRIORITY.—After having been notified, as provided in subparagraph (A), the Attorney General shall have the right—

(i) to file a civil action, subject to monetary limits equal to those set forth in section 3(c)(1);

(ii) to intervene in the action;

(iii) upon so intervening, to be heard on all matters arising therein;

(iv) to remove the action to the appropriate United States district court; and

(v) to file petitions for appeal.

(D) PREEMPTION.—

(i) ACTION BY DEPARTMENT OF JUSTICE.—If the Attorney General institutes a civil action or intervenes in an action under this subsection, the functional regulator, a State attorney general, or an official or agency of a State may not bring an action under this section for any violation of this Act alleged in the complaint.

(ii) ACTION BY FUNCTIONAL REGULATOR.—If the functional regulator institutes a civil action or intervenes under sec-

tion 3(d)(1) to enforce compliance with section 3, a State attorney general or official or agency of a State, may not bring an action under this section for any violation of this Act alleged in the complaint.

(b) LIMITATIONS ON STATE ACTIONS.—

(1) VIOLATION OF INJUNCTION REQUIRED.—A State may not bring an action against a person under subsection (a)(1)(C) unless—

(A) the person has been enjoined from committing the violation, in an action brought by the State under subsection (a)(1)(A); and

(B) the person has violated the injunction.

(2) LIMITATION ON DAMAGES RECOVERABLE.—In an action under subsection (a)(1)(C), a State may not recover any damages incurred before the date of the violation of an injunction on which the action is based.

(c) CONSTRUCTION.—For purposes of a civil action under subsection (a), nothing in this Act shall be construed to prevent the attorney general of a State from exercising the powers conferred on such attorney general by the laws of that State to—

(1) conduct investigations;

(2) administer oaths or affirmations; or

(3) compel the attendance of witnesses or the production of documentary and other evidence.

(d) VENUE; SERVICE OF PROCESS.—

(1) VENUE.—Any action brought under subsection (a) may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

(2) SERVICE OF PROCESS.—In an action brought under subsection (a), process may be served in any district in which the defendant—

(A) is an inhabitant; or

(B) may be found.

SEC. 5. EFFECT ON STATE LAW.

The provisions of this Act shall supersede any law, rule, or regulation of any State or unit of local government that relates in any way to electronic information security standards or the notification of any resident of the United States of any breach of security pertaining to any collection of personal information about such resident.

SEC. 6. EFFECTIVE DATE.

This Act shall take effect on the expiration of the date which is 180 days after the date of enactment of this Act.

Calendar No. 252

109TH CONGRESS
1ST SESSION

S. 1326

A BILL

To require agencies and persons in possession of computerized data containing sensitive personal information, to disclose security breaches where such breach poses a significant risk of identity theft.

OCTOBER 20, 2005

Reported without amendment